UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* four cellphones previously seized by the Glendale Police Department (GPD) during the arrest of Terry OWENS Jr. during a traffic stop on July 11, 2024.	)	Case No.24-895M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 9/20/2024 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. xx❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued:9/6/2024 @ 10:20 a.m.

Nancy Joseph

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched are four cellphones previously seized by the Glendale Police Department (GPD) during the arrest of Terry OWENS Jr. during a traffic stop on July 11, 2024:

1) A black in color iPhone in a pink and white case, GPD item #24-001860-1

2) A black in color iPhone, GPD item # 24-001861-1

3) A black in color Cloud Mobile cellular phone, GPD item #24-001863-1

4) A black in color iPhone in a black case, GPD item #24-001862-1

ATTACHMENT B

Particular Things to be Seized

All records and information on the Devices described in Attachment A that relate to a violation of Title 21 U.S.C. § 841(a)(1) (possession with intent to and distribution of a controlled substance), Title 18 U.S.C. § 924(c) (firearm possessed in furtherance of drug trafficking), 18 U.S.C § 922(g) (possession of a firearm and ammunition by a convicted felon), and 26 U.S.C. § 5861(d) (possession of an unregistered firearm regulate under the National Firearms Act) occurring prior to and ending on July 11, 2024, including:

a. Preparatory steps taken in furtherance of these crimes as detailed and found in document files located on the Target Phones as well as the below listed locations thereon;

b. Any audio, video, and/or photograph(s) files on the phone of criminal activity or of evidentiary value;

c. All voicemail and call records;

d. All text messages;

e. All social media sites used and applications for social media sites;

f. All internet activity;

g. All location data including from the phone and/or from any downloaded applications;

b. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. Records evidencing the use of the Internet Protocol address to communicate, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

four cellphones previously seized by the Glendale Police Department (GPD) during the arrest of Terry OWENS Jr. during a traffic stop on July 11, 2024.

Case No.24-895M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	possession with intent to and distribution of a controlled substance
18 U.S.C. § 924(c)	firearm possessed in furtherance of drug trafficking
18 U.S.C. § 922(g)	possession of a firearm and ammunition by a convicted felon
26 U.S.C. § 5861(d)	possession of an unregistered firearm regulated under the National Firearms Act

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

PAUL KOZELEK
Digitally signed by PAUL KOZELEK
Date: 2024.08.30 11:42:30 -05'00'

Applicant's signature

Paul Kozelek, Special Agent - ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 9/6/2024

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

I, Paul Kozelek, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been since January of 2020. Prior to my employment with ATF, I was a Sheriff's Deputy with the Jackson County Sheriff's Office in Black River Falls, WI. My duties included patrol, drafting and executing search warrants, and investigations related to state and county criminal violations. Previous to my tenure with the Jackson County Sheriff's Office, I served with the United State Marine Corps from 2004 until 2008, and the United States Marine Corps Reserve from 2011 until 2014. I left the Marine Corps as an E6/Staff Sergeant holding the billet of Platoon Commander. I received my bachelor's degree in Criminal Justice Administration from Viterbo University, La Crosse, WI in 2016.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. I have previously applied for and received search warrants related to cell site data and other related cellphone company records.

5. This affidavit is based upon my personal knowledge as well as information provided to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and my training and experience. Through my experience and training as a firearm and arson investigator, I am aware that electronic devices, such as cellphones, can be used to store and save audio, video, and text files that can link to a variety of criminal activity. I am also aware that smart cellphones are capable of capturing location history for the device. I have previously applied for and received search and arrest warrants related to the crimes of arson and unlawful firearm possession, as well as other crimes. I know from training and experience that those that commit crimes commonly communicate, photograph, videotape, and organize using electronic devices, including by phone call, text message, electronic mail, messaging application, and social media.

6. As an ATF agent, I have participated in the investigation of firearms and narcotics-related offenses, resulting in the prosecution and conviction of individuals and the seizure of illegal drugs, and weapons. My experience has taught me how to distinguish between a personal user of controlled substances, a lower-level narcotic street dealer and a higher quantity, more complex drug trafficker. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of controlled substances. I am further keenly aware through experience that many drug traffickers carry firearms to protect

themselves, their narcotics, and their narcotic proceeds. Further, I know the following concerning cellular phone evidence in narcotics investigations:

7. Based on my training and experience, I know that individuals involved in narcotics trafficking often maintain more than one phone or more than one SIM card device to have multiple avenues to facilitate drug trafficking activities, and in an attempt to avoid detection by law enforcement. I am aware that individuals involved in drug trafficking often utilize prepaid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of third persons to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug trafficking often change SIM cards to make it difficult for law enforcement to determine their records. Based on my training and experience, I know that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

8. Based on my training and experience, I know that drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

9. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is

no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

10. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephone, are one of the few ways to verify the numbers (i.e., telephones, etc.) being used by specific traffickers.

11. In addition, I know that those involved with narcotics trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, i.e. photographs of accomplices and/or individuals common to co-conspirators. I am also aware that narcotics traffickers often take photographs or make videos of drugs, drug proceeds and firearms with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones to show to associates, and/or to upload to social media.

12. Furthermore, based on my training and experience and the training and experience of other agents, I know that drug traffickers often use a cellular phone’s internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an internet search engine to explore where banks or mail delivery services are located or may use

the internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephones internet browser to update their social networking sites to communicate with co-conspirators, and to display drugs and drug proceeds or to post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

13. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

14. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

15. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21 U.S.C. § 841(a)(1) (possession with intent to and distribution of a controlled substance), Title 18 U.S.C. § 924(c) (firearm possessed in furtherance of drug trafficking), 18 U.S.C § 922(g) (possession of a firearm and ammunition by a convicted felon), and 26 U.S.C. § 5861(d) (possession of an unregistered firearm regulated under the National Firearms Act) have

been committed by Terry OWENS Jr. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

16. The property to be searched are four cellphones previously seized by the Glendale Police Department (GPD) during the arrest of OWENS during a search on July 11, 2024: a black in color iPhone in a pink and white case, GPD item #24-001860-1 (**DEVICE 1)**, a black in color iPhone, GPD item # 24-001861-1 (**DEVICE 2)**, black in color Cloud Mobile cellular phone, GPD item #24-001863-1 (**DEVICE 3)**, black in color iPhone in a black case, GPD item #24-001862-1 (**DEVICE 4)**,

PROBABLE CAUSE

17. Your affiant reviewed Glendale Police Department (GPD) report #24-008407 which related to an incident that occurred on July 11, 2024, at approximately 5:00 PM in the 5400 block of N. Port Washington Rd. in the City of Glendale, in the Eastern District of WI. The following is a summary of the GPD report.

18. On July 11, 2024, at approximately 5:00 PM a GPD officer observed a 2006 Cadillac SRX, silver in color with no license plate traveling south on N. Port Washington Rd. The GPD officer conducted a traffic stop in the 5400 block of N. Port Washington Rd. The driver and sole occupant was identified as Terry R. OWENS Jr. (M/B DOB XX/XX/1988). OWENS claimed to have just purchased the vehicle that day. While interacting with OWENS, officers detected the

odor of marijuana. Officers reviewed OWENS' information and found that his driver's license was suspended, and he was a convicted felon and was on active felony probation.

19. Officers asked OWENS if he had smoked marijuana. OWENS denied and stated other people had smoked it. OWENS was placed under arrest. A second officer who had arrived observed "blunts" in the center cupholder, a scale and a clear plastic bag behind the front passenger seat. A "blunt" is a common term referring to a cigar which has been emptied and refilled with marijuana. The combination of these items are indicative of illegal drug use.

20. A search incident to arrest was conducted on the vehicle. The following is not a complete list of all items found, only those which provide probable cause for this affidavit:

1) Black in color iPhone with pink and white case which was plugged into a charging port on the dash (**DEVICE 1**);
2) Black in color iPhone found next to the gear shift (**DEVICE 2**);
3) Black ash tray holding the partially consumed "blunts" referred to in paragraph 19;
4) Green "Bucks" bag on the front passenger seat which contained: a total of $210.00 in US currency, a total of 7 grams of methamphetamine, a total of 14 grams of cocaine, WI driver license for OWENS, razor, rolling paper packaging, a paper business card with "Hemp 1848" and "3955 N 35th St.;
5) Black in color Cloud Mobile cellular phone found on the front passenger seat (**DEVICE 3**);
6) 2 scales;
7) "Good Times" brand rolling paper;
8) Marijuana grinder;
9) Red Solo cup with green substance located on the rear driver side floorboard;

10) Large opened plastic bag which contained 262 grams of marijuana on the rear passenger side floorboard;

11) Black in color iPhone in black case on the front passenger seat (**DEVICE 4**);

12) Multi-colored mylar bag containing marijuana residue on the front passenger seat;

13) In the glove box was a box of clear sandwich bags;

14) In the glove box was a Glock model 19, 9mm pistol bearing serial number; AGGK184, with an attached "auto sear" and an extended magazine loaded with 27 rounds of ammunition. (Note: an "auto sear" is a machine gun conversion device which attaches to the rear of a semi-automatic Glock type pistol and converts it into a fully automatic machinegun which is subject to the National Firearms Act);

15) A large quantity of mylar bags were located throughout the vehicle including the trunk area, front and rear passenger areas;

16) A large quantity of clear sandwich type bags were located throughout the vehicle including the truck area, front and rear passenger areas;

17) Glass jar which contained $49.00 of US currency in bills and $108.85 of coinage;

18) In the trunk was a "Oatmeal" box which contained: $500.00 in US currency, knotted clear plastic bag containing 1 gram of methamphetamine, clear knotted bag

which contained 1 gram of methamphetamine, plastic bag containing 15 grams of cocaine and an empty clear bag;

19) $2.96 in loose change; and

20) Located on OWENS' person was $4,123.14 in US currency.

21. The total currency found was $4,993.95. The total amount of illegal narcotics was 29 grams of cocaine, 8 grams of methamphetamine, and 262 grams of marijuana.

22. During a Mirandized interview, OWENS stated he was in the process of purchasing the Cadillac he was arrested in. He had stopped to get some food and was on his way home when he was stopped by officers. OWENS denied knowing about the narcotics or the firearm in the vehicle. When asked if OWENS would provide a DNA sample, he requested a lawyer. Officers ended the interview at that point.

23. The Glock model 19, 9mm pistol bearing serial number AGGK184 was found to be reported stolen. It was stolen on February 15, 2024, from 7200 W. Fond Du Lac Ave. in the City of Milwaukee, and documented in Milwaukee Police Department case #240480093.

24. Your affiant reviewed OWENS' criminal history and found the following felony convictions:

1) Milwaukee County case #2015CF003703 on 12-29-2015, Felony Bail Jumping
2) Milwaukee County case #2021CF004837 on 4-27-2023, Possession of firearm by a convicted felon.

CONCLUSION

25. As described within this affidavit, and based on the substantial quantity of marijuana, methamphetamines, cocaine, along with the type and quantity of packaging materials,

presence of scales, the large amount of cash, the possession of a stolen firearm which was modified to be a machinegun regulated under the NFA, your affiant believes that there is probable cause to show will be evidence of violations of Title 21 U.S.C. § 841(a)(1) (possession with intent to and distribution of a controlled substance), Title 18 U.S.C. § 924(c) (firearm possessed in furtherance of drug trafficking), 18 U.S.C § 922(g) (possession of a firearm and ammunition by a convicted felon), and 26 U.S.C. § 5861(d) (possession of an unregistered firearm regulate under the National Firearms Act) located on the four cellphones seized by GPD on July 11, 2024: a black in color iPhone in a pink and white case, GPD item #24-001860-1 (**DEVICE 1)**, a black in color iPhone, GPD item # 24-001861-1 (**DEVICE 2)**, black in color Cloud Mobile cellular phone, GPD item #24-001863-1 (**DEVICE 3)**, black in color iPhone in a black case, GPD item #24-001862-1 (**DEVICE 4)**

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing

back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera and video recorder, portable media player, internet web browser, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems

can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. As described above and in Attachment B, this application seeks permission to search and seize things that the TARGET TELEPHONES might contain, in whatever form they are stored. As used herein, the term "electronic device" includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephones.

32. Based on my knowledge, training, and experience, as well as information related to me by others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and in a variety of areas within the devices and thus the entire device must be searched. In particular, I know that electronic devices, including cellular telephones used by drug traffickers, are likely to be repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

33. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

34. Based on my knowledge, training, and experience, as well as information related to me by others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices. In particular, I know that electronic devices, including cellular telephones used by drug traffickers, are likely to be repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

35. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

36. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic devices and software programs in use today that specialized equipment is sometimes necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications that are being searched.

37. I am also aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

38. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials

contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment and can require substantial time.

39. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular data on an electronic device is not segregable from the electronic device. Analysis of the electronic device as a whole

to demonstrate the absence of particular data can require specialized tools and a controlled laboratory environment and can require substantial time.

40. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, law enforcement officers and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, law enforcement intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

41. *Manner of execution.* Because this warrant seeks only permission to examine the Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

The property to be searched are four cellphones previously seized by the Glendale Police Department (GPD) during the arrest of Terry OWENS Jr. during a traffic stop on July 11, 2024:

1) A black in color iPhone in a pink and white case, GPD item #24-001860-1

2) A black in color iPhone, GPD item # 24-001861-1

3) A black in color Cloud Mobile cellular phone, GPD item #24-001863-1

4) A black in color iPhone in a black case, GPD item #24-001862-1

ATTACHMENT B

Particular Things to be Seized

All records and information on the Devices described in Attachment A that relate to a violation of Title 21 U.S.C. § 841(a)(1) (possession with intent to and distribution of a controlled substance), Title 18 U.S.C. § 924(c) (firearm possessed in furtherance of drug trafficking), 18 U.S.C § 922(g) (possession of a firearm and ammunition by a convicted felon), and 26 U.S.C. § 5861(d) (possession of an unregistered firearm regulate under the National Firearms Act) occurring prior to and ending on July 11, 2024, including:

a. Preparatory steps taken in furtherance of these crimes as detailed and found in document files located on the Target Phones as well as the below listed locations thereon;

b. Any audio, video, and/or photograph(s) files on the phone of criminal activity or of evidentiary value;

c. All voicemail and call records;

d. All text messages;

e. All social media sites used and applications for social media sites;

f. All internet activity;

g. All location data including from the phone and/or from any downloaded applications;

b. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. Records evidencing the use of the Internet Protocol address to communicate, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.